International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 293-300
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Scheme based on Boolean Operations and Elliptic Curve Cryptography

Dr. K.Shankar[1], Dr. G. Devika[2], Dr. M. Ilayaraja[3]
Assistant Professor[1,2,3],
School of Computing,
Kalasalingam University,
Krishnankoil, – 626126, Tamil Nadu, India.
shankar.k@klu.ac.in[1], devika.g@klu.ac.in[2] , ilayaraja.m@klu.ac.in[3]

***Abstract*—The growth of network communication, secret sharing scheme is one of the best approaches to protect the secret images from the potential intruders while transmission over unsecured channel. Secret image sharing scheme is based on Boolean operation attained good in performance due to Exclusive-OR values computation. This is the main intent to develop the proposed scheme for (n, n)-Multi Secret Image Sharing scheme (MSIS) to generate multiple shares from the multiple secret images. In this proposed scheme, 'n' secret images are encoded into 'n' shared images based on XOR operations. In the existing schemes, hacker cannot guess the secret information directly with any single share. But there is a possibility of retrieval if hackers are able to collect the entire shares passing in sequence over the network. To resolve this issue multiple shares are encrypted by using Elliptic Curve Cryptography. Hence this proposed scheme provides high security for the multiple shares and multiple secret images. Moreover, the performance of the proposed scheme has been analyzed and evaluated through image quality parameters of the PSNR and CC. It offers secure and efficient scheme for multiple secret images and its shares.**

Keywords—Multi secret image secret sharing ; Shares; Boolean; XOR; PSNR;

I. INTRODUCTION

With the rapid development of multimedia data, it is important to maintain the confidentiality of such data. The sender transmits the secret data over unsecure channel which can be easily retrieved or 'damaged' by unauthorized entity. Once the confidential information is illegitimately retrieved, the unauthorized person makes use of the content for their own benefits. This main issue was solved in the year 1979, by Blakley in [1] and Shamir in [2] introduced the Secret Sharing (SS) schemes in which the secret data is partitioned into *n* shares and distributed to *n* participants with utmost confidentiality and availability. The *(k, n)* threshold schemes [3, 4, 5] possess some properties such as secret data which can be recovered only from *k* shares or more than *k* shares. In case, if any *k-1* or less than *k* shares request for access, the secret data cannot be recovered. To evaluate a secret sharing scheme, four conditions such as security, contrast, computational complexity and pixel expansion are used [1, 2, 7-9]. The schemes satisfying the security and recovering the original secret image is without any loss. Unfortunately, computational complexity is high in non-visual SS schemes. To eliminate this issue the VSS (Visual Secret Sharing) schemes were proposed in [6, 10, 18, 19] which uses the human visual system in order to share the visual data such as pictures, printed text, documents and also the computational complexity is low in this scheme. But there was a problem of pixel expansion since each original pixel is coded into *m* subpixels per shadow image. In 1987, the credit goes to Kafri, Oded, and Eliezer Keren for launching the concept of VSS based Random Grids (RG) in [13] without the absence of pixel expansion problem. Various researchers are also solved in [6, 11, 12] the aforementioned drawbacks by probabilistic visual schemes which has no computational complexity and also no pixel expansion. Even though this scheme provides a solution for pixel expansion and complexity problem, still it suffers from reconstruction precision. To overcome this issue, Cimato *et al.* [6] designed a generalized probabilistic scheme (ProbVSS) by performing two Boolean Exclusive operations, OR ($\oplus$) and AND (&) that allow to recover the secret image in lossless manner. The previous schemes are applicable only in case of binary images [10, 4]. After this the number of schemes are proposed for both grayscale images and 'numerical' color images in [12, 14-16, 18].

Wang *et al.* have proposed [17] a *(2, n)* scheme for binary images which is called Boolean-based VSS. In this scheme, Boolean AND & Exclusive OR operations are used to attain good performance with no pixel expansion and the original secret image is reconstructed entirely in decoding phase with low computational complexity. Many researchers proposed various schemes in order to protect only one shared image. A situation, where more than one image is sharing, there is need in improvisation of performance as well as security. For this purpose, the technique MSIS scheme is used to *'n'* images encoded into *'n'* secret shares. All *n* shares are must required to reconstruct original secret images. Lin *et al.* [35] given theoretical based calculations to share two secret images by employed operations stack / flip to reconstruct two images. Chen *et al.*[36] using the technique called fixed angle segmentation for creating circular shared images and stacked together all shared images at various angles to reveal the secret messages. Chen suggested [20] *(n,n)* SISS in which use the Boolean operations to encrypt *n-1* images among n shared images. Chen and Wu [21] have made improvisation on the

above scheme [20] by increase the capacity of sharing as well as security of shared images. While multi images are sharing, computational complexity is substantial one. Among various techniques, Boolean based operations helps to attain low computational complexity.

II. Review of Literature

Tzung-Her Chen *et al.* developed an algorithm [20] for *(n+1, n+1)* multi-secret sharing using XOR operations. In this scheme, '*n*' original data (image) is encoded into '*n+1*' meaningless shadow images and need all *n+1* share to restore all *n* secret images. Moreover, extra random matrix is used to create shared images. This advanced scheme provides some features such as Restoration of original image in lossless manner, absence of pixel expansion problem and also no codebook required. Computational cost is *O(m)*for n secret images.

Chien-Chang Chen *et al.*[21] has been proposed multi secret image sharing scheme on the basis of Boolean in which creating a random image among shares using a random image generated F function. Bit shift subfunction used to produce random image to meet requirements randomly. Moreover, proposed system has been analysed and evaluated, the results shows that the capacity of share is increased n/n and shares are random.

Ching-Nung Yang *et al.* [22] has been overcame the inaccuracy in Chen and Wu's (*n, n*)-MSIS scheme and improved the multi secret image sharing scheme based on Boolean. Chien-Chang Chen *et al.* [23] has been suggested novel multi-secret image sharing scheme based symmetric and Boolean operations like XOR, bit reverse, pixel shift, hash function etc., which enable to achieve the low complexity and met more randomness among shares.

Maroti Deshmukh *et al.* [24] has been developed Multi Secret Image Sharing Scheme on the basis of Boolean XOR and modular arithmetic. In this scheme, reverse bit function is applied to more randomness. Researchers suggested three methods to share the multi secret images. First two methods used XOR and reverse bit function for graylevel and color images. Third method used additive inverse and reverse bit operation.

Chunyan Song *et al.* [25] has been suggested novel encryption scheme using the combination of DNA and spatiotemporal chaos for protect the image. Xing-Yuan Wang *et al.* [26] has been proposed scheme using DNA and CML (Coupled Map Lattice). In this scheme, plain image has been confused and encoded it using DNA rules.

K.Shankar *et al.* [29] have been proposed new VSS algorithm for protecting image from adversaries using Elliptic Curve Cryptography with Optimization Technique. In this method, shares are created from the secret image and each share is given as input to encryption and decryption process by means of ECC algorithm. In encryption process, public key is generated randomly and in decryption process, private key is optimally generated using optimization techniques. Then, the concert of the image is taken as a fitness value to be considered as PSNR values. The author made performance comparison of the different optimization technique (PSO, ACO, CS, and GWO) is utilized to obtain the private key to the decryption process.

III. Properties of the Secret Image Sharing Schemes

The Visual Secret Sharing scheme, also known as the VSS, represents a confidential sharing model for images in which the decryption is carried out by superimposing the stacked shares through human visual mechanism [30]. In recent years, there are many VSS algorithms have been developed for secret sharing. Most of the algorithm exhibits the following disadvantages.

1) **Pixel Expansion:** Each pixel in the original image is mapped into 'm' pixels in shadow image which causes these shadow images to be of larger size and making their handling and storage, a challenging one.
2) **Reconstruction Accuracy:** The reconstructed image contrast is lesser than the original image contrast so the decryption process is difficult.
3) **Reconstruction Complexity:** It concerns the total number of operators required both to generate the set of 'n' shadows and to restructure the original secret image.
4) **Reconstruction Image Quality:** It is considered that the quality of recovered original image and it is evaluated by image quality measures such as PSNR, MSE etc.
5) **Shares Security:** Cheaters can collude among themselves to make bogus shadow to show a false secret and thus, it can cheat other secret holders [31].

IV. Problemstatement

A new-fangled secret sharing scheme is given another name called VSS scheme. It is a confidential dividing system that encrypts the original data (image) into numerous shadows. But to recover the original secret image, computational complexity is not required. Every shadow consists of an element of confidential image detail. But it suffers from pixel expansion problem (Each share m times as large as original image) and also low reconstruction accuracy.

Later, other VSS schemes have been proposed to resolve the above deficiency. But it suffers from the problem of high reconstruction complexity and low image quality. In addition to this, hackers cannot guess the secret information directly with any single shadow. So there is a possibility of retrieval if hackers are able to collect the entire shadow passing in sequence over the network. Hence this research work proposes multiple secret images shared with multiple secrets, that satisfies the lack of pixel development, elevated reconstruction accuracy, effortless reconstruction complexity, augment shadow security and enhancement of the reconstructed image quality all at the same time.

V. Proposed Methodology

The secret image is divided into shares and then transferred between the sender and receiver. Each share hides the secret image information and the entire shares are stacked together, then the secret image is clearly viewed and it gives the original images information to the receiver. It is called as the secret image sharing scheme. Earlier secret image sharing

schemes are shared only one secret image. With the continuous and exponential increase in the number of users, and their securely shared more number of secret images over the encrypted data in the online appears to be a challenging task. Hence this proposed multi-secret image sharing scheme is used to split a multiple secret image into multiple shares by using Boolean operations (XOR). It is very useful to preserve the reconstruction accuracy and low reconstruction complexity. It also helps to produce the shares with lack of pixel development. After shares are generated from the multiple secret images and then encrypt each share using public key cryptography. Here the secret shares are more secured and protected from the malicious adversaries who can alter the bit sequences to create the fake shares.

To enhance the security of shares, ECC algorithm is used even though hackers are able to get all the shadow images, they cannot retrieve the original secret without the private key access [32]. To examine the confidentiality of the image and broadcast procedure of SIS Scheme along with ECC utilized to encrypt and decrypt the shares with high reconstructed image quality evaluate by PSNR and CC. In this section, the proposed method has been well-defined and clearly illustrated with step of instructions.

A. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography based on the arithmetic model of elliptic curve with limited fields. Due to the differentiation in ECC, it required smaller keys than other public key algorithm to yield equivalent protection. Public key cryptosystems are necessary for the acknowledgement of contemporary encryption or advanced signature tactics. One secret key is used as the 'decoding key' or 'signature creation key' and the other, analogous key is used as the 'cipher text generation key' or 'signature confirmation key'. Without the correct key, the encrypted source content finds it hard to detect, even though unauthorized person can steal the data [33]. For a long time, elliptic curves are studied by several mathematicians which is an algebraic curve whereas elliptic curve is a plane curve defined by the equation,

$$y^2+b_1xy+b_2y=x^3+a_1x^2+a_2x+a_3$$

Graphical representation of the elliptic curve is shown in figure 2.1. The curve of this nature is called elliptic curve.
The following equation represents the elliptic curve over real numbers,

$$y^2=x^3+ax+b$$

The ECC is a sensible, protected technology to be utilized in constrained applications. Generating curves are used as cryptographic curves which must go through many algorithms and procedures so as to make a constant cryptographic curve. The main purpose of using elliptic curves are smaller key sizes and more capable enough to be utilized at the same security level alike the extra broadly deployed policies such as RSA [34].

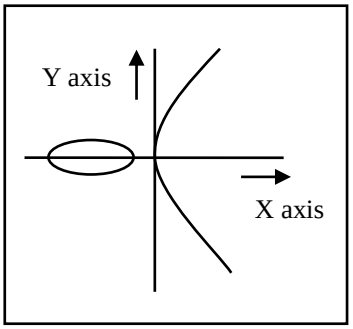

Figure 2.1: A Simple Elliptic Curve.

B. Algorithm: Proposed Multi Secret Image Sharing Scheme - Sharing Procedure.

Input: *n* secret images $\{I_1, I_{2,\dots} I_n\}$.
Output: *n* shared images $\{S_1, S_{2,\dots} S_n\}$
Step 1: Read the multiple secret color images.
Step 2: Extract the color components from all the secret images

$$I_n = \{I_1, I_{2,\dots} I_n\} = \begin{Bmatrix} (I_{r1}, I_{g1}, I_{b1}), \\ (I_{r2}, I_{g2}, I_{b2}) \dots \\ (I_{rn}, I_{gn}, I_{bn}) \end{Bmatrix}$$

Step 3: Perform the following XOR calculation between the secret images with separate color components to obtain the scrambled image $F_1 = (F_{rn}, F_{gn}, F_{bn})$

$$F_{rn} = (I_{r1} \oplus I_{r2} \oplus \dots \oplus I_{rn})$$
$$F_{gn} = (I_{g1} \oplus I_{g2} \oplus \dots \oplus I_{gn})$$
$$F_{bn} = (I_{b1} \oplus I_{b2} \oplus \dots \oplus I_{bn})$$

Step 4: Compute function F_2 using bit complement operation on F_1.

$$F_2 = \sim F_1$$

Example: $F_1 = 11100010$ *then* $F_2 = 00011101$

Step 5: Generate multiple shared images

$$Share\_1 = (I_{r1} \oplus F_2, I_{g1} \oplus F_2, I_{b1} \oplus F_2)$$
$$Share\_2 = (I_{r2} \oplus F_2, I_{g2} \oplus F_2, I_{b2} \oplus F_2)$$
$$Share\_n = (I_{rn1} \oplus F_2, I_{gn} \oplus F_2, I_{bn} \oplus F_2)$$

Step 6: To enhance the shares security elliptical curve cryptography (ECC) based encryption method is applied on multiple shares. In ECC method,

$$x = y(i)^3 + p * x(i) + q$$

Where, *p* and *q* are the constants and it is *p=q=2.*

Step 7: If the condition *a=b* is satisfied, the best point is selected for the elliptic curve. The *a* and *b* is

$$a = mod(E, n_p)$$
$$b = mod((bp(j)^2, n_p)$$

Where, *bp* (i, j) is the points of the elliptic curve. n_p is the prime number.

Step 8: The doubling process is used to find the *a* and *b* values. The best point $P_e(k,l)$ and P_f is the public key. The public key P_f is the

$$P_f = H \times P_e$$

Step 9: In the ECC encryption method, each share converted into 8×8 block and every block is encrypted by the encryption method of ECC. The number of blocks are represented as *pixel(i, j)* where i and j are the row and column of the block of the share. In the encryption process, the every two pixel of the image given as input.. The pixels of $D_x(i, j)$ and $D_y(i+1,j)$ and the point is

$$C_1 = H \times P_e$$
$$C_2 = (D_x, D_y) + C_1$$

Step 10: The above process (Step 6 to 9) repeated to encrypt the multiple shares from the multiple secret images.

C. Algorithm: Proposed Multi Secret Image Sharing Scheme – Recovering Procedure.

Input: *n* shared images $\{S_1, S_{2,\ldots} S_n\}$

Output: *n* recovered secret images $\{I_1, I_{2,\ldots} I_n\}$.

Step 1: Read the multiple encrypted share images.

Step 2: To decrypt the encrypted multiple shares by using decryption process of the ECC Method. In the decryption process, the private key (H) is used to decrypt the pixels and the point C_3 is used decrypt the pixel point.

$$C_3 = H \times C_1$$
$$C_{ij} = C_2 - C_3$$

The C_{ij} represents the decrypted shares. This process is repeated to decrypt the multiple encrypted shares.

Step 3: Compute function F_2 using XOR operation between the all shares.

$$F_2 = Share_1 \oplus Share\_2 \oplus \ldots . Share\_n$$

Step 4: Compute function F_1 using bit complement operation on F_2.

$$F_1 = \sim F_2$$

Step 5: Recover the secret images with separate color component wise.

$$I_1 = Share\_1 \oplus F_2$$
$$I_2 = Share\_2 \oplus F_2$$
$$I_n = Share\_n \oplus F_2$$

D. Example: Construct and Reconstruct multiple secret images (2 secret images- Take 1 pixel value)

1. Construct multiple secret images

Step 1: Secret Image1= I_1=10

Step 2: Secret Image2= I_2=20

Step 3: Compute function

$$F_1 = I_1 \oplus I_2 = 10 \oplus 20 = 30$$

Step 4: Convert binary equivalent of $F_1 = 00011110$

Step 5: Complement operation is used to compute function $F_2 = \sim F_1 = 11100001 =$ 225 $(Decimal\ equivalent)$

Step 6: Generate share1:

$$Share_1 = I_1 \oplus F_2 = 10 \oplus 225 = 235$$

Step 7: Generate share2:

$$Share_2 = I_2 \oplus F_2 = 20 \oplus 225 = 245$$

Step 8: ECC Algorithm to encrypt share 1:

$$Enc_{Share_1} = 145$$

Step 9: ECC Algorithm to encrypt share 2:

$$Enc\_Share_2 = 59$$

2. Reconstruct multiple secret images

Step 1: Encrypted share 1: $\text{Enc\_Share}_1 = 145$

Step 2: Encrypted share2: $\text{Enc\_Share}_2 = 59$

Step 3: ECC Algorithm to decrypt the share1: $\text{Share}_1 = 235$

Step 4: ECC Algorithm to decrypt the share2: $\text{Share}_2 = 245$

Step 5: Compute function

$$F_1 = \text{Share}_1 \oplus \text{Share}_2 = 235 \oplus 245 = 30$$

Step 6: Convert binary equivalent of $F_1 = 00011110$

Step 7: Complement operation is used to compute function $F_2 = \sim F_1 = 11100001 = 225$ (Decimal equivalent)

Step 8: Reconstruct secret image1:

$$I_1 = \text{Share}_1 \oplus F_2 = 235 \oplus 225 = 10$$

Step 9: Reconstruct secret image2:

$$I_2 = \text{Share}_2 \oplus F_2 = 245 \oplus 225 = 20$$

VI. RESULTS AND DISCUSSION

The proposed scheme is implemented in Visual Studio 2010, C# language under the configuration of windows 7 operating system with Core-i3 and 3 GB RAM. The overall performance of the proposed scheme is analysed by using the Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC).

A. Experimental Results

In this section, experiments are carried out on proposed (*n*, *n*) Boolean-based multi-secret image sharing scheme with various secret images such as the Lena, Sailboat, Peppers and Jet. The images were obtained from USC-SIPI Image Database [27].

(a) I_1

(b) I_2

(c) I_3

(d) I_4

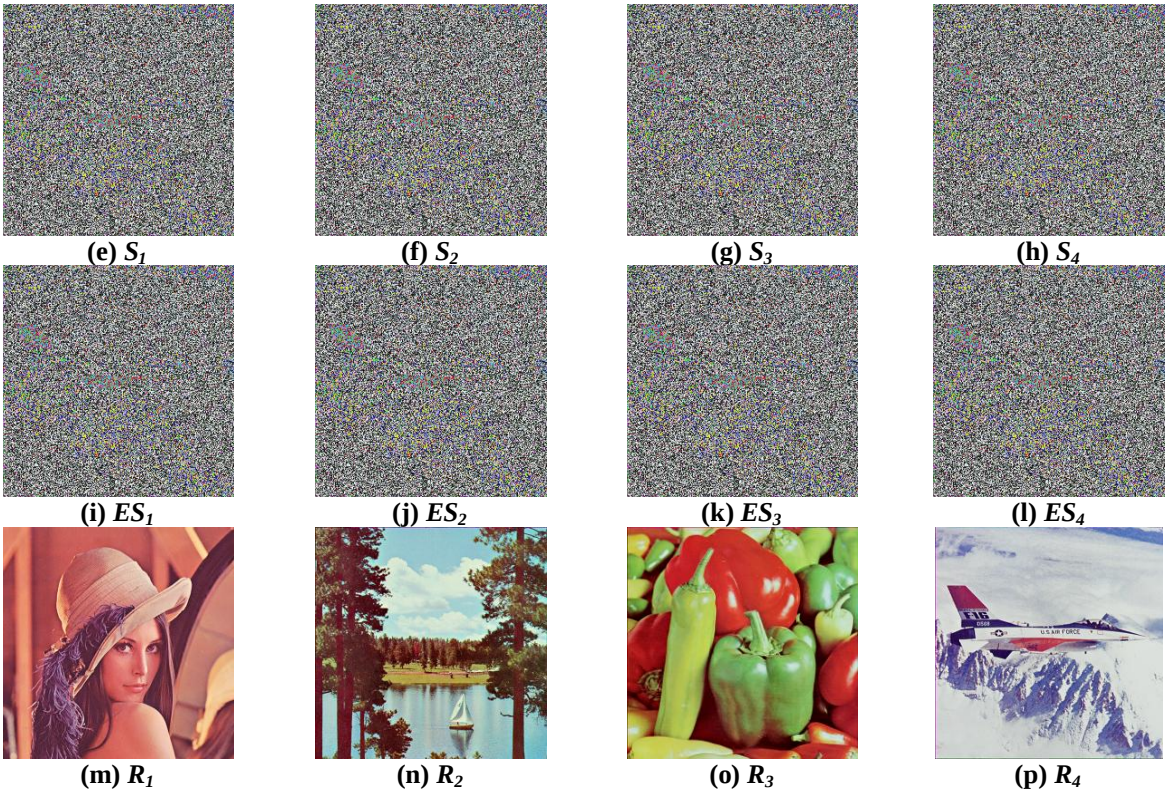

Fig. 1. Results of the proposed scheme (a-d) Secret images (I_1, I_2, I_3, I_4). (e-h) Shared Image (S_1, S_2, S_3, S_4). (i-l) Encrypted Shares Images (ES_1,ES_2,ES_3,ES_4) Recovered images (R_1,R_2,R_3,R_4).

B. Performance Analysis

1) PSNR: The Peak Signal to Noise Ratio is defined as the ratio between the maximum possible power of the signal and the power of the corrupted noise.

$$PSNR = 20 * \log_{10}(255/\sqrt{MSE})$$

Where, MSE is the mean square error value of the image. Therefore, it is highly essential to take utmost care regarding the extent of validity of this metric. The table 1 shows the PSNR values of different secret images and its recovered images.

It is clear that the PSNR values between original image and decrypted images are high; it represents proposed method provides high quality of the secret images [28].

TABLE I
PSNR Results between Original and Recovered Secret Images

Secret and Recovered image	PSNR
I_1, R_1	54.65
I_2, R_2	52.74
I_3, R_3	54.78
I_4, R_4	55.14

2) Correlation Coefficient (CC): Correlation is often a measure of the bonding between a pair of variables. To analyze the correlation involving two adjacent pixels throughout plain-image as well as ciphered image, this process has been executed. Initially, randomly choose 1000 pairs associated with two adjacent (in horizontal, vertical, and diagonal direction) pixels from an image. Next, compute the correlation coefficient of each one set through the subsequent equations,

$$G(p) = \frac{1}{F_p}\sum_{l=1}^{F_p}(p_l - M(p))^2$$

$$M(p) = \frac{1}{F_p}\sum_{l=1}^{F_p}P_l$$

$$CON(p,q) = \frac{1}{F_p}\sum_{l=1}^{F_p}((p_l - M(p)) * (q_l - M(q)))$$

$$W(p,q) = \frac{CON(p,q)}{\sqrt{M(p) * M(q)}}$$

where, $W(p,q)$ is the correlation coefficient, $M(p)$ and $M(q)$ are the mean value of the P_l and q_l and both values are $\neq 0$. p_l and q_l are the two adjacent pixel values; F_p is the number of pairs (p,q).

TABLE II
CC Results between Original and Recovered Secret Images

Secret and Recovered image	CC
I_1, R_1	0.999848
I_2, R_2	0.999918
I_3, R_3	0.999885
I_4, R_4	0.999879

To analyze the correlation involving two adjacent pixels throughout input image as well as recovered image, the CC has been used. The CC results are shown in the table 2. The proposed schemes have the maximum CC value which is

nearly 1 and it represents the original image is maintained in the recovered image after the suggested segment.

C. Comparative Analysis

The proposed (n, n) MSIS is compared with many other existing schemes [20, 21, 22, 24] are listed in Table 3. It shows a broader-level comparison among the existing SIS schemes and the proposed schemes on the basis of some important constraints such as Number of Secret Images, Number of Shared Images, Pixel Expansion, Recovery Type, Recovery Strategy, Sharing Type, Color Depth, Sharing Capacity and Shadow Security. The conceptuality of SIS scheme is that in case if a pixel is expanded after encoding an original image, an algorithm seems to have high complexity. Also the time taken for transmission is too high over the unsecured public communication medium because of size of the enlarged encoded image when compared to secret image size. To overcome these kind of issues, different authors designed various algorithm that has no pixel expansion problem, by implementing some operations such as Boolean etc.,

TABLE III FEATURE COMPARISONS AMONG THE PROPOSED SCHEME AND OTHER RELATED SCHEMES

Schemes	Secret Images	Shared Images	Pixel Expansion	Recovery Type	Recovery Strategy	Sharing Type	Color Depth	Sharing Capacity	Shadow Security
Propsoed Scheme	*n*	*n*	No	Lossless	*XOR*	Rectangle	Grayscale and color	*n/n*	Yes
Ref. [20]	*n*	*n+1*	No	Lossless	*XOR*	Rectangle	Grayscale	*n/n+1*	No
Ref. [21]	*n*	*n*	No	Lossless	*XOR*	Rectangle	Grayscale	*n/n*	No
Ref. [22]	*n*	*n*	No	Lossless	*XOR*	Rectangle	Grayscale	*n/n*	No
Ref. [24]	*n*	*n*	No	Lossless	*XOR*	Rectangle	Grayscale and color	*n/n*	No

In many existing approaches, reconstructed image in contrast loss manner, while there is absence of pixel expansion problem and also the quality of the recovered image is low. Furthermore, shadows are transmitted in the form of actual share and so unauthorized entities can't reveal the secret with any 'one' shadow but there may be a chance that it can gather all shadows. Thus, to resolve this issue, the proposed approach needs enhancement in security. In order to improve it, shadows are encrypted with the help of ECC public key cryptography encoding algorithms in this proposed schemes. Many SIS's are applicable to binary, grayscale and color images. But some algorithms are applied to Grayscale, while some are applied for color images or color image only or grayscale only or binary image only. In Table 3, the proposed scheme proves to be effective in terms of recovering lossless image, low complexity and improved recovered image quality (PSNR= 55.14), no expansion of pixel and improved security of shadows.

VII. CONCLUSION

This research work proposed a secure and efficient multi-secret image sharing scheme based on boolean operations and elliptic curve cryptography. The proposed multi-secret image sharing scheme with assist of ECC algorithm is used to secure the multiple secret images from the unintended receipient. In traditional secret image sharing scheme schemes, it is highly complex and challenging to maintain the shares information. This predominant issue is solved in this research work with the help of ECC.The performance analysis and experimental results of this research study promote the proposed scheme attained less computation and high security with high sensitivity on shared images in *MSIS*. The possibility of improving this scheme by utilizing different encryption methodlolgy to secure the shares for further research.

ACKNOWLEDGMENT

The author would like to thank the management of Kalasalingam University, Krishnankoil, Tamilnadu, India, for the facilities provided to carry out this research work.

REFERENCES

[1] G. Blakley, "Safeguarding crypographic keys", presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, page(s): 313–317, June 1997.

[2] Adi Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, page(s): 612–613, 1979.

[3] Simmons and Gustavus J, "An introduction to shared secret and/or shared control schemes and their application", Contemporary cryptology: The science of information integrity, page(s): 441–497, 1992.

[4] H. Zheng, "Linear threshold schemes, visual cryptography, and parasitehost cryptosystems", Ph.D. Dissertation of the Texas A&M University, 1998.

[5] Stinson and Douglas R, "An explication of secret sharing schemes", Designs, Codes and Cryptography, vol. 2, issue.4, page(s): 357–390, 1992.

[6] Cimato, Stelvio, Roberto De Prisco, and Alfredo De Santis, "Probabilistic Visual Cryptography Schemes", The Computer Journal, vol. 49, No. 1, page(s): 97–107, 2006.

[7] Ateniese, Giuseppe, et al. "Extended capabilities for visual cryptography", Theoretical Computer Science, vol.250, issue.1, page(s): 143–161, 2001.

[8] Chang, Chin-Chen, and Ren-Junn Hwang, "Sharing secret images using shadow codebooks", Information Sciences, vol. 111, issue.1, page(s): 335–345, 1998.

[9] Ito, Mitsuru, Akira Saito, and Takao Nishizeki, "Secret sharing scheme realizing general access structure", Electronics and Communications in Japan (Part III: Fundamental Electronic Science), vol. 72, issue.9, page(s): 56–64, 1989.

[10] M. Naor and A. Shamir, "Visual cryptography" in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, page(s): 1–12, Springer-Verlag, LNCS.

[11] Ching-Nung Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, vol. 25, issue.4, page(s): 481–494, 2004.

[12] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no. 10, page(s): 2172–2177, 1999.

[13] Kafri, Oded and Eliezer Keren, "Encryption of pictures and shapes by random grids", Optics letters, vol. 12, issue.6, page(s): 377–379, 1987.

[14] C.Blundo, A.DeBonis, and A.DeSantis, "Improved schemes for visual cryptography", Designs, Codes and Cryptography, vol. 24, page(s): 255–278, 2001.

[15] Yang, Ching-Nung, "A note on efficient color visual encryption", J. Inf. Sci. Eng. 2002.

[16] C. N. Yang and C. S. Laih, "New Colored Visual Secret Sharing Schemes", Designs, Codes and Cryptography, vol.20, page(s): 325–335, 2000.

[17] Daoshun Wang, Lei Zhang, Ning Ma and Xiaobo Li, "Two secret sharing schemes based on Boolean operations", Pattern Recognition, vol. 40, issue.10, page(s): 2776–2785, 2007.

[18] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition, vol. 36, page(s): 1619–1629, 2003.

[19] Ching-Nung Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, vol. 25, issue.4, page(s): 481–494, 2004.

[20] Tzung-Her Chen and Chang-Sian Wu, "Efficient multi-secret image sharing based on Boolean operations", Signal Processing, vol. 91, issue.1, page(s): 90–97, 2011.

[21] Chen, Chien-Chang, and Wei-Jie Wu. "A secure Boolean based multi-secret image sharing scheme." Journal of Systems and Software 92 (2014): 107-114.

[22] Yang, Ching-Nung, Cheng-Hua Chen, and Song-Ruei Cai. "Enhanced Boolean-based multi secret image sharing scheme." Journal of Systems and Software (2015).

[23] Chien-Chang Chen, Wei-Jie Wu, Jun-Long Chen, "Highly efficient and secure multi-secret image sharing scheme", Multimedia Tools and Applications, Volume 75, Issue 12, pp 7113–7128, June 2016.

[24] Deshmukh, Maroti, Neeta Nain, and Mushtaq Ahmed. "An (n, n)-multi secret image sharing scheme using boolean XOR and modular arithmetic." Advanced Information Networking and Applications (AINA), 2016 IEEE 30th International Conference on. IEEE, 2016.

[25] Song, Chunyan, and Yulong Qiao. "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos." entropy 17.10 (2015): 6954-6968.

[26] Wang, Xing-Yuan, Ying-Qian Zhang, and Xue-Mei Bao. "A novel chaotic image encryption scheme using DNA sequence operations." Optics and Lasers in Engineering 73 (2015): 53-61.

[27] http://www.hlevkin.com/TestImages

[28] Shankar, K., and P. Eswaran. "Sharing a secret image with encapsulated shares in visual cryptography." Procedia Computer Science 70 (2015): 462-468.

[29] K.Shankar and Dr.P.Eswaran, "A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique", Australian Journal of Basic and Applied Sciences, Vol.9, Issue.36, pp:150-163, 2015.

[30] Xiaotian Wu and Wei Sun, "Improved tagged visual cryptography by random grids", Signal Processing, vol. 97, page(s): 64–82, 2014.

[31] Mishra, Sonu K., and Kumar Biswaranjan, "Robust Cheat-prevention for Random Grids Based Visual Secret Sharing Scheme", Procedia Computer Science, vol.46, page(s): 517–523, 2015.

[32] Kulvinder Kaur and Vineeta Khemchandani, "Securing Visual Cryptographic shares using Public Key Encryption", Advance Computing Conference (IACC), 2013 3rd IEEE International Advance Computing Conference (IACC), page(s): 1108–1113, 2013.

[33] Tsaur and Woei-Jiunn, "Several security schemes constructed using ECC-based self-certified public key cryptosystems", Applied Mathematics and Computation, vol. 168, issue 1, page(s): 447–464, 2005.

[34] Joppe Bos, Alex Halderman, Nadia Heninger, Jonathan Moore and Michael Naehrig, "Elliptic Curve Cryptography in Practice", Journal of Financial Cryptography and Data Security, Vol.157, pp.1–16,2013.

[35] Sian-Jheng Lin, Shang-Kuan Chen and Ja-Chen Lin, Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion, Journal of Visual Communication and Image Representation,Vol. 21, page(s): 900–916, 2010.

[36] Jeanne Chen; Tung-Shou Chen; Hwa-Ching Hsu; Hsiao-Wen Chen, New visual cryptography system based on circular shadow image and fixed angle segmentation, Journal of Electronic Imaging, Vol.14, No.3,page(s): 033018-033018, 2005.

K.Shankar is an assistant professor in the Department of Computer Science and Information Technology at the Kalasalingam University, Krishnankoil, Tamilnadu, India. He received his master degrees of Master of Computer Applications, Master of Philosophy in Computer Science and Ph.D. degree in computer science from Alagappa University, Karaikudi, India. He has several years of experience working in the research, academia and teaching. His current research interests include Cryptography and Network Security, Cloud security, Image Processing and Soft Computing Techniques.

The author Dr. M. Ilayaraja, Assistant Professor, Department of Computer Science & Information Technology, Kalasalingam University, Krishnankoil. He has completed his doctoral degree in the area of data mining. He has been very much interest in doing research in the area of data mining and network security. He was published various papers related to heart disease prediction and information security. He has been familiar in working with some of the data mining tools. He also developed some methods to predict the risk of heart diseases by analyzing large volume of medical datasets and also developed various methods to secure the information over public transmission medium.

G. Devika is an assistant professor in the Department of Computer Science and Information Technology at the Kalasalingam University, Krishnankoil, Tamilnadu, India. She received her Ph.D. degree in computer science from Anna University, India. She has several years of experience working in the research, academia and teaching. Her current research interests include Cryptography and Network Security, Cloud computing, and Image Processing.